

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

TRISTRATA, INC.,
Plaintiff,
v.
MICROSOFT CORPORATION, et al.,
Defendants.

Case No. 11-cv-03797-JST

**ORDER CONSTRUING CLAIM
TERMS, DENYING MOTION TO
STRIKE TECHNOLOGY TUTORIAL,
AND GRANTING MOTION TO
SUPPLEMENT RECORD ON CLAIM
CONSTRUCTION**

Before the Court are the parties' competing constructions of several claim terms contained in U.S. Patent Nos. 7,257,706 ("the '706 patent'") and 7,743,249 ("the '249 patent'"), which the Court now construes pursuant to Markman v. Westview Instruments, Inc., 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc), aff'd, 517 U.S. 370 (1996), and Patent Local Rule 4–3. Also before the Court are Defendants' Motion to Strike Portions of TriStrata's Technology Tutorial, ECF No. 100, which the Court will deny, and Plaintiff's Motion to Supplement the Record on Claim Construction, ECF No. 123, which the Court will grant.

I. BACKGROUND

A. Relevant Cryptography Background

The study of securely transmitting information from one party to another is known as cryptography. Cryptographers develop methods and tools for obscuring the contents of a document or communication so that third parties cannot know its contents. One such tool is encryption, the process through which a document, which begins as readable in "plaintext," is converted into "ciphertext," an indecipherable collection of characters. Ciphertext is converted back to plaintext through decryption. Encryption and decryption are accomplished via algorithms — mathematical functions that evaluate plaintext or ciphertext alongside a "key" in order to

1 translate from one to the other. Encryption and decryption keys are typically alphanumeric
2 strings, or, more fundamentally, strings of bits that, when evaluated by the algorithm, convert
3 plaintext into ciphertext and vice versa.

4 A rudimentary (and easily reverse-engineered) encryption algorithm might convert each
5 letter of plaintext into a letter of ciphertext by first assigning a numeric value to each letter of the
6 alphabet, then adding to the plaintext character's numerical value the number provided by the key,
7 and then converting the value back to a letter. If, for example, the key is "3," each "A" would
8 become a "D," each "J" would become an "M," each "Z" would become a "C," and so on.
9 (Algorithms, of course, get more complicated, but the basic concepts remain the same.) The
10 algorithm is the lock, and only the keys that fit will open it, revealing the locked container's
11 contents.

12 In digital cryptography, encryption algorithms, or ciphers, are so complex that only
13 computers can encrypt and decrypt data. Keys likewise are long enough to make it difficult, if not
14 impossible, to try every possible key combination in an effort to circumvent the encryption.
15 Indeed, encryption algorithms can be, and often are publicly known and understood without
16 compromising the security of information encrypted using them.

17 There are two types of keys: symmetric and asymmetric. Symmetric keys can be used
18 both to encrypt and decrypt the same content. The example key above is a symmetric key: to
19 encrypt, the "3" is added to the letter's numeric value; to decrypt, it is subtracted. For symmetric
20 keys to work, the sender and receiver of the secure information must have the key, which means
21 they must arrange beforehand to share it with each other.

22 Symmetric keys become less useful at a large scale. For example, in order for any two
23 individuals to communicate securely, they each would need the same symmetric key, and they
24 would have had to exchange it in a secure manner prior to communicating. If a third person joins
25 the group, and each of the original two desires to communicate with the third without the other
26 eavesdropping, each pair of potential communicators would need a unique symmetric key. In a
27 group of three people, there are three unique pairs. In a group of five, there are ten. In a group of
28 ten thousand, there are 49,950,000.

1 Since users may want to communicate with other users prior to actually meeting them and
2 exchanging a symmetric key, a central trusted authority, often a server, is required to pool the keys
3 and distribute them to the users using a scheme sometimes called a Kerberos system. This creates
4 a key distribution problem, though: the management of all the keys necessary to maintain a large
5 network with a constantly changing composition is unwieldy and unreliable, as it depends entirely
6 on the availability of the central server and the ability of that server to know who in the network
7 desires access to others. In a corporate network, that task might be manageable; on the scale of the
8 entire Internet, it is practically impossible. In addition, symmetric key schemes become more
9 complicated when users desire to communicate with multiple users at once. Finally, the reliability
10 and integrity of the scheme relies entirely on the reliability and integrity of the Kerberos server. If
11 the server is compromised, the system breaks down.

12 Asymmetric keys are one way to solve the key distribution problem. Asymmetric keys
13 either encrypt or decrypt, which means that two asymmetric keys are required for any one
14 transmission: one to encrypt and a second to decrypt. One use of asymmetric keys is in public-
15 private encryptions schemes, which are akin to conventional mailboxes. The public key
16 corresponds to an address; the private, to the mailbox key. Anyone with the recipient's public key
17 can encrypt a message for the recipient, but the message cannot be decrypted with that key, just as
18 a member of the public cannot access mail already delivered through a locked mail slot, even if
19 they know the recipient's address. Instead, only the recipient can decrypt the message, by using
20 the private key that only the recipient has, just as the mail recipient uses a key to open the mailbox
21 and retrieve the mail.

22 A similar asymmetric key scheme is a digital signature system, whereby a sender's private
23 key is used to generate a signature, which accompanies the transmission. The signature can only
24 be verified by using that sender's public key, not unlike authentication of a letter via a wax seal.
25 If, after the public key is applied to the algorithm, the signature does not compute correctly, the
26 recipient knows the identity of the sender, or the integrity of the transmission itself, cannot be
27 verified.

28 Although public-private key schemes obviate the need for sender and recipient to meet

1 beforehand to exchange a key, they introduce another problem: the integrity of the message can be
2 compromised if the public key does not actually correspond to its intended owner, but rather to a
3 bad actor that has intercepted the communication and, by distributing a different public key, has
4 surreptitiously convinced the user that it is the intended recipient of the communication. The
5 solution, known as public-key infrastructure (“PKI”), involves the use of independent third parties,
6 known as certificate authorities, who can certify the authenticity of public keys. As long as the
7 third party certificate authority authenticates the public key in a satisfactory manner, i.e. in person,
8 or otherwise offline in a manner that sets aside any legitimate question of authenticity, and, as
9 long as the certificate authority retains the public’s trust, PKI remains workable. In fact, the
10 public keys for the most popular Internet servers are distributed with Internet browsers, or with an
11 operating system, making the process even simpler. PKI is commonly used to secure online
12 banking, online shopping, and other highly sensitive online activities.

13 Encryption schemes are usually used in combination with one another to establish secure
14 transmissions and send and receive secure communications. For example, an internet server and a
15 computer user may first utilize a public-private key scheme to establish a private access line
16 (“PAL”), after which messages may be sent back and forth securely with confidence that the
17 sender and recipient are who they say they are. Further, once the PAL is established, the internet
18 server may send the user encrypted content, such as a video stream, that the user may only decrypt
19 by using the appropriate key, depending on whether the user is authorized to view the content.
20 One way for the server to make the determination is to distribute a symmetric key that corresponds
21 to the video stream. But then anyone could share the key with unauthorized users, who could then
22 view the stream, too.

23 Another method could involve public-private key encryption, whereby the internet server
24 uses the public key for each intended viewer to encrypt the stream, and the viewer decrypts the
25 stream using the viewer’s private key. The weakness of that approach is that the server must
26 encrypt the symmetric key that decrypts the stream separately for each intended viewer, and either
27 send the stream individually for each user, or send it all as one package of encrypted symmetric
28 keys, forcing the user either to look for the right public key among the encrypted symmetric keys,

1 or to refer to a list of users who have access to determine which encryption is the right one, which
2 means the access list is public to anyone who downloads the file.

3 **B. Patents-in-Suit**

4 The two patents-in-suit, U.S. Patents 7,257,706 (“the ‘706 patent’”) and 7,743,249 (“the
5 ‘249 patent’”) are both titled “Method of Securing a Document in a System and Controlling
6 Access to the Document and a Seal for Use in the Method.” They are the final two patents in a
7 series of five patents assigned to TriStrata concerning the security of computer documents: U.S.
8 Patents 5,960,086 (“’086 patent”) (Atalla, 1995); 6,088,449 (“’449 patent”) (Atalla, 1996);
9 6,912,655 (“’655 patent”) (Zucker, 1999); the ’706 patent (Zucker, Atalla, Adams, 2005); and the
10 ’249 patent (Zucker, Atalla, Adams, 2007). The last three patents share a common specification,
11 as each is a continuation of the last.¹ Each patent also incorporates the earlier patents in the series
12 by reference. Finally, the 1999 patent also incorporates abandoned patent application number
13 09/095,350. The patents-in-suit are directed at the problems associated with broadcast (one-to-all)
14 and multicast (one-to-many) transmissions described above. In particular, the ’706 and ’249
15 patents claim a “method for efficient multicast key management.” ’706 patent, col. 2:22–23; ’249
16 patent, col. 2:25–26.

17 **II. LEGAL STANDARD**

18 The construction of terms found in patent claims is a question of law to be determined by
19 the court. Markman v. Westview Instruments, Inc., 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc),
20 aff’d, 517 U.S. 370 (1996). “[T]he interpretation to be given a term can only be determined and
21 confirmed with a full understanding of what the inventors actually invented and intended to
22 envelop with the claim.” Phillips v. AWH Corp., 415 F.3d 1303, 1316 (Fed. Cir. 2005) (quoting
23 Renishaw PLC v. Marposs Societa' per Azioni, 158 F.3d 1243, 1250 (Fed. Cir. 1998)).
24 Consequently, courts construe claims in the manner that “most naturally aligns with the patent's
25 description of the invention.” Id.

26 The first step in claim construction is to look to the language of the claims themselves. “It
27

28 ¹ Because they share a specification, the Court will focus on the ’706 patent where appropriate.

1 is a ‘bedrock principle’ of patent law that ‘the claims of a patent define the invention to which the
2 patentee is entitled the right to exclude.’” Phillips, 415 F.3d at 1312 (quoting Innova/Pure Water,
3 Inc. v. Safari Water Filtration Sys., Inc., 381 F.3d 1111, 1115 (Fed. Cir. 2004)). A disputed claim
4 term should be construed in light of its “ordinary and customary meaning,” which is “the meaning
5 that the term would have to a person of ordinary skill in the art in question at the time of the
6 invention, i.e., as of the effective filing date of the patent application.” Phillips, 415 F.3d at 1312.
7 In some cases, the ordinary meaning of a disputed term to a person of skill in the art is readily
8 apparent, and claim construction involves “little more than the application of the widely accepted
9 meaning of commonly understood words.” Id., at 1314. Claim construction may deviate from the
10 ordinary and customary meaning of a disputed term only if (1) a patentee sets out a definition and
11 acts as his own lexicographer, or (2) the patentee disavows the full scope of a claim term either in
12 the specification or during prosecution. Thorner v. Sony Computer Entm't Am. LLC, 669 F.3d
13 1362, 1365 (Fed. Cir. 2012).

14 Ordinary and customary meaning is not the same as a dictionary definition. “Properly
15 viewed, the ‘ordinary meaning’ of a claim term is its meaning to the ordinary artisan after reading
16 the entire patent. Yet heavy reliance on the dictionary divorced from the intrinsic evidence risks
17 transforming the meaning of the claim term to the artisan into the meaning of the term in the
18 abstract, out of its particular context, which is the specification.” Id., at 1321. Typically, the
19 specification “is the single best guide to the meaning of a disputed term.” Vitronics Corp. v.
20 Conceptronic, Inc., 90 F.3d 1576, 1582 (Fed. Cir. 1996). It is therefore “entirely appropriate for a
21 court, when conducting claim construction, to rely heavily on the written description for guidance
22 as to the meaning of claims.” Phillips, 415 F.3d at 1315. However, while the specification may
23 describe a preferred embodiment, the claims are not necessarily limited only to that embodiment.
24 Id.

25 Finally, courts may consider extrinsic evidence in construing claims, such as “expert and
26 inventor testimony, dictionaries, and learned treatises.” Markman, 52 F.3d at 980. Expert
27 testimony may be useful to “provide background on the technology at issue, to explain how an
28 invention works, to ensure that the court's understanding of the technical aspects of the patent is

1 consistent with that of a person of skill in the art, or to establish that a particular term in the patent
2 or the prior art has a particular meaning in the pertinent field.” Phillips, 415 F.3d at 1318.

3 However, extrinsic evidence is “less reliable than the patent and its prosecution history in
4 determining how to read claim terms.” Id. If intrinsic evidence mandates the definition of a term
5 that is at odds with extrinsic evidence, courts must defer to the definition supplied by the former.

6 Id.

7 **III. CLAIM TERM CONSTRUCTIONS**

8 The ’706 and ’249 patents are directed at an “efficient multicast key management” scheme
9 that “is achieved by using seals.” ’706 patent, abs.; ’249 patent, abs. Four of the patents in the
10 five-patent series use the term “seals.” Nothing in any of the five patents explicitly defines the
11 term despite its central role in the patent claims.

12 The specification shared by the patents-in-suit teaches that secure broadcast and multicast
13 transmissions are difficult to accomplish by using (1) conventional, or symmetric, encryption, or
14 (2) PKI cryptography. The former is unwieldy and insecure; the latter leads to the multicast key
15 management problems discussed above. See ’706 patent, col. 1:23–2:16. As in symmetric
16 encryption, the distribution and maintenance of encryption keys in PKI cryptography in a
17 broadcast context becomes “difficult and impractical.” Id. 2:16.

18 The summary of invention discloses a system that involves “the transmission of what are
19 called ‘permits’ and ‘seals’ to allow the storage of secured documents and the accessing of secured
20 documents by authorized clients or for secured messaging between clients.” Id. 2:26–30. “[T]he
21 security server generates what is called a ‘seal.’” The “seal” may contain a key or information to
22 generate a key. Id. 2:32–35. “The security server encodes this key or information to generate this
23 key using any encryption method. The encoded key is called a ‘seal’ which is generated by the
24 security server.” Id. 2:35–36. The seal may also contain a user identification code, “a policy
25 which is a description as to who is allowed access to what,” a message digest made up of a hash of
26 files, or a date and time stamp. Id. 2:32–45. “The key or the information to generate the key is
27 often called a ‘permit,’ so the permit is contained within the seal but may not be the exclusive
28 contents of the seal.” “All the information contained in a seal is encrypted by the security server

1 and can only be ‘opened,’ i.e., decrypted, by the security server which encrypted the seal.” Id.
2 2:46–49.

3 The broadcast transmission scheme disclosed by the patents includes three sets of actors:
4 security servers, application servers, and application clients. The latter two may be, for example, a
5 web server and a web user, or a database and a database client. Id. 2:53–56. The application
6 server requests a seal from the security server. The security server returns one, and the application
7 server “then broadcasts the seal to a plurality of application clients. Each client wishing to encrypt
8 or decrypt a data stream sends the seal it received from the application server to the security server
9 in an open seal request signal, together with the client’s identification information, so that the seal
10 can be ‘opened.’” Id. 2:59–66. The security server “decrypts the seal and compares the client’s
11 identification with the policy stored at the security server.” Id. 2:57–3:1. If the policy provides
12 for access by the client, the security server “extracts a permit from the decrypted seal and
13 transmits the permit to the client in clear text form.” Id. 3:2–4. The client can then use the permit
14 to encrypt or decrypt the data stream. In this manner, the patents “solve[] the broadcast key
15 distribution problem.” Id. 7:64–65.

16 The parties dispute the proper construction of a number of claim terms, most important of
17 which is the parties’ dispute over the meaning of the term “seal.”

18 **C. “seal”**

Claim Term	TriStrata’s Proposed Construction	Microsoft’s and Adobe’s Proposed Construction
<p>19 “seal” 20 All claims</p>	<p>21 Information in the form of computer 22 bits used by a computer system to 23 secure documents through encryption. 24 The seal contains information relating 25 to an encryption/decryption key, such 26 as information from which the key can be derived or the key itself.</p>	<p>27 An encrypted data structure 28 generated by a security server and containing a key or information to generate a key, wherein the entire data structure is symmetrically encrypted and decrypted only by the security server that created it.</p>

27 **i. Intrinsic Evidence**

28 In construing disputed claim terms, the Court first looks to the language of the claims

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

themselves. The term “seal” appears in most of the ’706 and ’249 patents’ claims. Relevant recitations include:

’706 Patent

Claim 1: A method of securing a document stored in a computer system which is part of a network, comprising:

- creating a seal associated with a document which is to be stored or shared within the computer system or network:
 - placing in the seal information identifying the person requesting that the document be secured (hereinafter the “requestor”); and
 - placing in the seal information identifying who can access the document;
- thereby allowing one or more designated persons to have access to the document in accordance with the information in the seal.

Dependent Claim 2: The method as in claim 1 wherein said seal includes a unique key.

Dependent Claim 3: The method of claim 2 further comprising sending said key to the requestor so that the key can be used by the requestor to encrypt the document.

* * *

Claim 14: A method for sealing and controlling access to a document stored or communicated in a computer system which is part of a network which comprises:

- creating a seal as part of a document which remains a part of the document when the document is in storage or when the document is sent in communication or is shared anywhere within the computer system or network; and
- encrypting said seal using a unique key at a server:
- said seal allowing the system to validate the requestor, and identify those authorized by the requestor to have access to the document.

* * *

Claim 28: A seal for sealing and controlling access to a document stored or communicated in a system which is part of a network, said seal comprising selected information . . . wherein said seal is encrypted using a unique key at a server”

’249 Patent

Claim 1: A system for securing a document stored in a computer system which is part of a network, comprising:

- a storage device storing a seal for association with a document which is to be stored or shared within the computer system or network, said seal comprising;

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- a) information identifying a requestor requesting that the document be secured; and
- b) information identifying one or more parties qualified to access the document.

Because the patents-in-suit are continuations of the '665 patent, and because they incorporate by reference the '449 patent, those patents' claims and specifications are also relevant intrinsic evidence. See In re Katz Interactive Call Processing Patent Litig., 639 F.3d 1303, 1325 (Fed. Cir. 2011) (“[W]e ordinarily interpret claims consistently across patents having the same specification. . . .”); Cook Biotech Inc. v. Acell, Inc., 460 F.3d 1365, 1377 (Fed. Cir. 2006) (reference to same claim term in prior art “was intended to refer to the same structures” where later patent incorporated prior art by reference).

The term “seal” first appears in the '449 patent, the second of the five patents in the series, which claims a method of securing the transmission of information through a key management scheme that involves digital signatures. The specification first uses the term “seals” in the context of a particular embodiment as follows: “The server will establish a private access line (“PAL”) which provides I.D. and authentication between the client and the security server. The system allows the transmission of what is called permits and seals to allow the storage of secured documents and the accessing of secured documents by authorized clients or for secured messaging between clients.” '449 patent, col. 9:58–64. That patent does not contain a definition of the term, though claim 17, which recites a method of encrypting information through the use of “pointers,” or data that points to specific byte addresses, refers to the term “seal” as collectively referring to two encrypted pointers, which are transmitted along with the document.

The '655 patent, titled “Network Security Architecture System Utilizing Seals,” contains the same specification as those in the patents-in-suit. In addition to the use of the term “seal” in that specification, independent claim 6 recites “[a] method of key management, comprising: generating a set of encrypted seal bits at a security server; transmitting said set of encrypted bits” from the security server to an application server, and several other steps. Independent claim 11 recites “[a] method for opening a seal, wherein said seal comprises a set of encrypted bits comprising information for generating a set of encryption/decryption bits.”

1 **ii. Ordinary and Customary Meaning**

2 The Court must construe disputed claim terms as having “the meaning that the term would
3 have to a person of ordinary skill in the art in question at the time of the invention.” Phillips, 415
4 F.3d at 1312. Ordinary and customary meaning can only be ascertained “after reading the entire
5 patent. It is the specification that serves as “the single best guide to the meaning of a disputed
6 term.” Vitronics, 90 F.3d at 1582.

7 Claim construction is not an exercise conducted in a vacuum, “but in the context of the
8 entire patent, including the specification.” Phillips, 415 F.3d at 1313. Thus, even where terms do
9 not, standing alone, have a customary meaning in the art, if a person of ordinary skill in the art
10 could derive the term’s meaning after reading the entire patent, then the ordinary meaning, as
11 interpreted by the person of ordinary skill, controls. See Honeywell Int’l Inc. v. Universal
12 Avionics Sys. Corp., 488 F.3d 982, 990 (Fed. Cir. 2007) (where claim terms had no ordinary
13 meaning to a skilled artisan, patent provided necessary context to define the term) (citing Irdeto
14 Access., Inc. v. Echostar Satellite Corp., 383 F.3d 1295, 1300 (Fed. Cir. 2004)).

15 Here, the parties agree that the term “seal” had no ordinary and customary meaning in the
16 art at the time of invention. See Wecker Decl. ISO TriStrata’s Claim Constructions, ECF No. 59,
17 Ex. 11 at 193:14–21 (July 13, 2013 Deposition of Donald Adams) (“We took the name ‘seal’ from
18 the old wax seal that was put on physical objects.”); Wesenberg Decl. ISO Microsoft’s Claim
19 Constructions, ECF No. 66-1, Ex. A p. 13 (Mazières Expert Report); id., Ex. B ¶ 22 (Rubin Expert
20 Report); Belloli Decl. ISO Adobe’s Claim Constructions, ECF No. 65, Ex. C ¶ 22 (Rubin Expert
21 Report).

22 TriStrata argues that its construction is consistent with the ordinary meaning of “seal” as
23 derived from a general-purpose dictionary, i.e., “something that secures (as a wax seal on a
24 document).” TriStrata maintains that the intrinsic evidence demonstrates “nothing was intended to
25 be conveyed by the term [“seal”] other than the common sense meaning of something that protects
26 a message.” ECF No. 58 p.8. Tristrata’s reliance upon a dictionary definition is problematic,
27 however, for a number of reasons.

28 First, Tristrata’s proposed construction is much narrower than the broad dictionary

1 definition, “something that secures.” It is not clear that one follows from the other.

2 Second, even if general-purpose dictionaries supported Tristrata’s construction, the Federal
3 Circuit has rejected the use of dictionary definitions without regard to the language of the patent.
4 “[H]eavy reliance on the dictionary divorced from the intrinsic evidence risks transforming the
5 meaning of the claim term to the artisan into the meaning of the term in the abstract, out of its
6 particular context, which is the specification.” Phillips, 415 F.3d at 1321. Thus, the Phillips court
7 held, claim terms must be construed in light of and only after reading the entire patent. Indeed, “in
8 the absence of something in the written description and/or prosecution history to provide explicit
9 or implicit notice to the public — i.e., those of ordinary skill in the art — that the inventor
10 intended a disputed term to cover more than the ordinary and customary meaning revealed by the
11 context of the intrinsic record, it is improper to read the term to encompass a broader definition
12 simply because it may be found in a dictionary, treatise, or other extrinsic source.” Nystrom v.
13 TREX Co., Inc., 424 F.3d 1136, 1145 (Fed. Cir. 2005).

14 Defendants, relying on Irdeto, 383 F.3d at 1300, argue that disputed terms that lack
15 customary meaning in the art must be construed “only as broadly as provided for by the patent
16 itself.” The patentee’s failure expressly to define the term “seal,” argue Defendants, merits a
17 departure from the “heavy presumption” in favor of construing claim terms according to their
18 ordinary meaning.

19 The patentee in Irdeto claimed “a system for controlling the broadcast of digital
20 information signals by using three layers or tiers of complementary encryption and decryption
21 keys.” Id. at 1296. The specification of the patent-in-suit consistently used the term “group,” in
22 the phrase “group key,” to refer to a subset of all subscribers of the satellite television service.
23 The plaintiff asserted that the term applied to a group of all subscribers, based on the ordinary
24 meaning of the term “group.” The Federal Circuit held that the specification limited the ordinary
25 meaning by the repeated and consistent implication that “group keys” are keys shared by a subset
26 of subscribers.² The Irdeto court also noted that “where evidence such as expert testimony or

27 _____
28 ² Also relevant to the Federal Circuit’s decision in Irdeto, and absent in this case, was the
applicant’s communication with the patent office demonstrating an intent to act as a lexicographer

1 technical dictionaries demonstrates that artisans would attach a special meaning to a claim term or
2 would attach no meaning at all to the claim term independent of the specification, ‘general-usage
3 dictionaries are rendered irrelevant with respect to that term’” Id. at 1300 (quoting
4 Vanderlande Indus. Nederland BV v. Int’l Trade Comm’n, 366 F.3d 1311, 1321 (Fed. Cir. 2004)).

5 Here, the term “seal” has a plain English meaning. The parties agree that the term was not
6 customarily used in the art, but rather was adapted by the inventor for use in cryptography as a
7 metaphor for physical, wax seals. A person of ordinary skill, after reading the entire patent, would
8 understand, first, that the term is used in the claims and the shared specification as an analog for
9 wax seals, but in a manner that has been adapted to fit the needs of the claimed invention. The
10 plain and ordinary meaning of the term “seal” that a skilled artisan would derive from the patent
11 specification has certain, specific limitations: namely, (1) the seal must be an encrypted data
12 structure, (2) it must contain a key or information to generate a key, and (3) it must be encrypted
13 by a security server, and capable of decryption only by the server that generated it. Those
14 limitations are evident from the patents themselves, and they are essential to the term as it is used
15 in the patents’ claims.

16 **iii. Limitations**

17 a. Encrypted Data Structure

18 The claims themselves provide no definitions, or even context from which a definition can
19 be derived, of the term “seal.” They do clarify that a seal will, at a minimum, contain two pieces
20 of information: the identity of the requestor, and information identifying who can access the
21 document. However, the summary of the invention makes clear that a seal, as disclosed by the
22 patents-in-suit, is an encrypted data structure. Where the specification discloses non-exclusive
23 embodiments, it uses the phrase “In one embodiment,” or “In another embodiment.” By contrast,
24

25 in the first instance. Id. (“[The] applicant informed the examiner and all competitors that the
26 “key” modifiers — ‘service,’ ‘group,’ and ‘box’ — have no accepted meaning in the art and ‘are
27 very adequately described in the specification.’ The applicant’s use of those terms in the
28 specification thus controls their scope.”). However, the Irdeto court’s decision did not rest on that
factor, as it found that the patent’s context defined the term even absent the express disavowal
normally required for Thorner redefinition.

1 in discussing the security server/application server/application client scheme described above, the
2 specification contains no such disclaimers. Instead, the entire scheme is described following the
3 preface: “In accordance with this invention,” ’706 patent, col. 2:50.

4 The patents claim a method whereby the seal is unreadable, and unusable, by anyone but
5 the security server that created it. The specification repeatedly teaches that security servers
6 “open” seals, unpack their contents, and return to the user the appropriate information or data. See
7 id. 2:65, 3:20. “All the information contained in a seal is encrypted by the security server and can
8 only be ‘opened,’ i.e. decrypted by the security server that encrypted the seal.” Id. 2:46–49. If the
9 seal were not encrypted, the security scheme would not function, and the security server would
10 serve no purpose, as it would be transmitted in plaintext. Indeed, the claims themselves, which
11 recite methods of securing documents, contain nothing other than the term ‘seal’ that relates to the
12 actual encryption of a document.

13 TriStrata argues that every limitation identified by Defendants is derived from a non-
14 limiting embodiment. For example, TriStrata argues that one of the paragraphs discussing the
15 encryption of seals also contains the phrase “In one embodiment,” see id. 2:31–49, rendering the
16 remainder of the paragraph non-limiting. A plain reading of the paragraph yields the opposite
17 conclusion: though it discloses three embodiments, it also teaches that, in any embodiment, the
18 contents of the seal are encrypted by the security server and can only be opened by it.

19 TriStrata also argues that even if the keys contained in the seal must be encrypted, other
20 pieces of information in the seal need not be encrypted, and suggests that, at most, the seal must be
21 partially, but not necessarily completely encrypted. The Court agrees. Indeed, the patent
22 discusses several types of information that may be contained in a seal, some of which, such as
23 permits, must be encrypted, and others of which, such as date and time stamps, need not be. In
24 addition, the patent specifically provides for the encryption of seals by security servers “using any
25 encryption method,” not just symmetrical encryption. Id. 2:35–36. Defendants’ proposed
26 construction must therefore be amended to read: “A data structure generated by a security server
27 and containing a key or information to generate a key, wherein part or all of the data structure is
28 encrypted and decrypted only by the security server that created it.”

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

b. Contains a Key, or Information to Generate a Key

The seal contains a key, or information that can be used to generate a key. TriStrata disputes this limitation even though its own proposed construction includes: “The seal contains information relating to an encryption/decryption key, such as information from which the key can be derived or the key itself.” TriStrata does not explain what, if any other types of information other than the key itself and information used to generate it may be contained in a seal. Instead, Plaintiff argues that nothing disclaims “other embodiments that may be devised to allow the seal of the Patents to accomplish its purpose of protecting documents.” ECF No. 58 p. 15. That argument is not persuasive. The limitation as proposed by Defendants adequately encompasses the broadest possible scope disclosed by the specification.

c. Generation, Encryption, and Decryption by Security Server

For the same reasons that seals must be encrypted data structures, they must be generated by a security server, encrypted by the security server, and decrypted by the same security server. The patents disclose that precise method in general terms, not as non-limiting embodiments. Nothing in the patents suggests that seals could be generated in another way, or that they could be encrypted by one entity and decrypted by another. The specification specifically forecloses that possibility: “All the information contained in a seal is encrypted by the security server and can only be ‘opened,’ i.e., decrypted, by the security server which encrypted the seal.” ’706 patent, col. 2:46–49.

iv. TriStrata’s Motion to Supplement the Record on Claim Construction

After the claim construction hearing, TriStrata moved to supplement the record on claim construction with a document Microsoft produced in discovery after the hearing occurred. ECF No. 123. Microsoft opposed the request on procedural and substantive grounds. The Motion is hereby GRANTED.

However, having reviewed the document, the Court concludes that it does not alter the Court’s claim construction analysis. The document is Microsoft’s MS Digital Asset Server Digital Rights Management Specification for eBooks (“DAS specification”). It concerns unrelated, proprietary Microsoft technology. The document defines the term “Seal/Unseal” in the context of

1 eBooks as: “Act of exposing or hiding Symmetric Keys required to encrypt/decrypt and use
2 protected eBooks.” “Sealed eBooks” are defined as: “Encrypted during the conversion to the .lit
3 file. It ensures the authenticity of content, meaning that the text and other content cannot be
4 modified. . . .” A “Sealed Copy” is defined as “An eBook that has been encrypted with a
5 Symmetric Key, which has been itself encrypted with a cryptographic hash of the metadata in the
6 title. . . .”

7 TriStrata makes two conflicting arguments about the DAS specification. First, TriStrata
8 argues that the document uses the word “seal” in a way that “clearly evok[es] the meanings [of]
9 the term as defined in the general purpose dictionaries.” ECF No. 123 at 2. Second, TriStrata
10 argues the document “clearly demonstrates that skilled artisans around the time of the patent
11 application used the term in the very fashion that TriStrata has [has] claimed.” ECF No. 126 at 1.

12 The Court is not persuaded by either contention. With regard to TriStrata’s “dictionary
13 definition” argument, the Court has concluded that the patentee did not intend to use the term
14 “seal” in the same way that the term is defined in a general purpose dictionary. Moreover, even
15 TriStrata’s proposed construction of the term is not consistent with a general purpose dictionary
16 definition. Rather, an appropriate construction is one that relies on the language of the
17 specification. Nothing in the Microsoft document changes that fact; in fact, the DAS specification
18 does not use the term “seal” in accordance with the general purpose dictionary definition, either.

19 With regard to TriStrata’s second argument, the Court notes that the definitions in the DAS
20 specification themselves contain limitations that are either inapposite here, or that are inconsistent
21 with TriStrata’s proposed construction. For example, “Seal” is defined as the act of hiding a
22 symmetric key. A “Sealed eBook” must be encrypted with a symmetric key, and then encrypted
23 again using the cryptographic hash from metadata, while TriStrata argues that a seal need not be
24 completely encrypted at all, and argues against the limitation of the term “seal” as requiring
25 symmetric encryption. And eBooks themselves appear in each definition, which are obviously
26 unrelated to the patents-in-suit. In short, the DAS specification document is not helpful to the
27 Court.

28 For the foregoing reasons, the Court therefore construes the term “seal” as: “A data

1 structure generated by a security server and containing a key or information to generate a key,
2 wherein part or all of the data structure is encrypted and decrypted only by the security server that
3 created it.”

4 **D. “key”**

Claim Term	TriStrata’s Proposed Construction	Microsoft’s and Adobe’s Proposed Construction
5 “key” 6 ’706 patent, claims 2, 3, 4, 7 11, 14, 17, 18, 25, 28 8 ’249 patent, claims 2, 3, 4	9 Cryptographic string of computer 10 bits used in an encryption/ 11 decryption process to make data 12 unreadable without access to the 13 key.	14 A secret string of bits with 15 which a message can be 16 encrypted and subsequently 17 decrypted.

18 Unlike the term “seal,” the term “key” unquestionably has an ordinary and customary
19 meaning in the art, which is accurately captured by TriStrata’s proposed construction. As
20 described above, keys can be symmetric or asymmetric. Nothing in the claims, the patents, or
21 extrinsic evidence suggests that the patentee acted as his own lexicographer in using the term
22 “key.” To the contrary, the term is used frequently throughout the patents, which themselves
23 explain the difference between symmetric and asymmetric keys.

24 Defendants’ proposed construction seeks to limit the term to symmetric keys that are
25 secret. Nothing in the claims themselves supports that position, nor does a full reading of the
26 patents suggest that, each time the patentee used the term “key” in the patent claims, the patentee
27 intended to limit the term to symmetric keys, even though throughout the specification and prior
28 art the term is used to mean one or both of symmetric and asymmetric keys.

The Court agrees, however, that TriStrata’s construction is unnecessarily confusing, as it
suggests that decryption can make data unreadable. In addition, it fails to account for the
difference, if there is any, between a “cryptographic” string of bits and an ordinary string of bits.
The Court therefore construes the term “key” as follows: “A string of bits used in encryption to
make data unreadable, or in decryption to render encrypted data readable.”

E. “encrypt”

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Claim Term	TriStrata’s Proposed Construction	Microsoft’s and Adobe’s Proposed Construction
“encrypt” '706 patent, claims 14, 28	Disguise a message in such a way as to hide its substance from someone not permitted to have access to the message.	Use a key to disguise a message in such a way as to hide its substance from those who do not know the key.

The parties’ proposed constructions of “encrypt” are virtually identical, but each suffers from a significant flaw. TriStrata’s proposed construction fails to account for the possibility that someone not permitted to have access to the message may nevertheless be able to read it by obtaining unauthorized access to a method of decrypting it. Defendants’ construction limits encryption to symmetric encryption, which limitation is not supported by the patent. Otherwise, the parties appear to agree that encryption is the process of disguising information from those who do not have the key necessary to decrypt it. The Court therefore construes the term “encrypt” as follows: “To disguise information such that it is unreadable to anyone who does not have the key necessary to decrypt it.”

F. “information identifying who can access the document” and “information identifying who can/one or more parties qualified to access the document”

Claim Term	TriStrata’s Proposed Construction	Microsoft’s and Adobe’s Proposed Construction
“information identifying who can access the document” “information identifying who can/one or more parties qualified to access the document” '706 patent, claims 1, 6, 16, 20, 25, 28 '249 patent, claims 1, 7	Information that identifies one or more persons who are permitted to have access to the document.	Plain and ordinary meaning in view of the intrinsic record and knowledge of one of ordinary skill.

The parties disagree as to the scope of the terms “information identifying who can access

1 the document,” as found in the ’706 patent, and “information identifying who can access the
2 document,” and “information identifying one or more parties qualified to access the document,” as
3 found in the ’249 patent. TriStrata seeks to exclude from the terms information identifying
4 categories or classes of people, as opposed to information identifying specific users. TriStrata
5 does not identify anything in the patents to support its proposed limitation. Nothing in the patents
6 limit the concept to the identification of individuals rather than individuals who are part of larger
7 groups. Indeed, the ’706 patent twice, in nearly identical language, explains that “[t]he policy ...
8 is a description as to who is allowed access to what (e.g., classification of files and security levels
9 of clients), which is consistent with information identifying categories or classes of users.” ’706
10 patent, col. 2:39–41, 6:65–67 (emphasis added).

11 The Court agrees with Defendants that a plain meaning construction is appropriate. A
12 person of ordinary skill in the art would understand the meaning of the disputed terms, and would
13 also understand that they may apply to information identifying classes of people, or individual
14 people, depending on the application.

15 **G. “information which allows the computer system to confirm server identity”**

Claim Term	TriStrata’s Proposed Construction	Microsoft’s and Adobe’s Proposed Construction
“information which allows the computer system to confirm server identity” ’706 patent, claims 13, 27 ’249 patent, claim 13	Information that allows the computer system to verify server identity information.	Pointers that are exchanged to establish the private access line that provides authentication and identification between the client and the security server.

16
17
18
19
20
21
22
23
24 Defendants propose to import several limitations into the term “information which allows
25 the computer system to confirm server identity” as it appears in the ’706 and ’249 patents, based
26 on one embodiment discussed in the specification of the ’706 patent. See ’706 Patent, col. 5:51–
27 54. The patents-in-suit do not define the term, and nothing in the patent suggests that the patentee
28 intended to limit the term to the embodiment Defendants rely upon. Indeed, the beginning of the

1 subject paragraph disclaims any such limitation. See id. 5:44 (“In one embodiment of the ’449
2 patent . . .”). Moreover, as Plaintiff argues, U.S. Patent Application No. 09/095,350, an
3 abandoned application incorporated by reference into the specifications of the patents-in-suit,
4 describes a different method for confirming server identity. See U.S. Patent Application No.
5 09/095,350, Wecker Decl. ISO Pl.’s Opening Claim Construction Brief, ECF No. 59, Ex. 8, pp.
6 14:22–16:13 (describing method for authenticating server and sender identities).

7 The Court adopts Tristrata’s construction of this term: “Information that allows the
8 computer system to verify server identity information.”

9 **H. Means Plus Function Claims**

10 The parties dispute whether claim 4 of the ’249 patent is indefinite.³

11 When claims use the term “means” to describe a limitation, they are presumed to be
12 means-plus-function limitations. Altiris, Inc. v. Symantec Corp., 318 F.3d 1363, 1375 (Fed. Cir.
13 2003). See 35 U.S.C. § 112 ¶ 6. Claim 4 recites: “The system of claim 3 further including means
14 for allowing the requestor to discard the key following the encryption of the document.” TriStrata
15 concedes that claim 4 is a means-plus-function claim. In construing such claims, “(1) the court
16 must first identify the function of the limitation; and (2) the court must then look to the
17 specification and identify the corresponding structure for that function.” Biomedino, LLC v.
18 Waters Technologies Corp., 490 F.3d 946, 950 (Fed. Cir. 2007). “[I]n order for a means-plus-
19 function claim to be valid under § 112, the corresponding structure of the limitation must be
20 disclosed in the written description in such a manner that one skilled in the art will know and
21 understand what structure corresponds to the means limitation. Otherwise, one does not know
22 what the claim means.” Id. If the patent does not disclose structure corresponding to the means-
23 plus-function limitation, the system claim is invalid as indefinite. Id.

24 Defendants argue that claim 4 is invalid as indefinite pursuant to 35 U.S.C. § 112 ¶ 2, for
25 failure to disclose a structure corresponding to the claimed function. TriStrata argues that the ’086
26 patent, incorporated by reference by the ’249 patent, discloses sufficient structure because it

27
28 ³ TriStrata concedes Adobe’s proposed identifications of structure pertaining to claims 3, 5, and 6
of the ’249 patent. ECF No. 70 p. 14.

1 explains that keys are used only once. The '249 patent likewise discloses a method for encryption
2 of a data stream with a key “to be used only once and then changed in a manner which is
3 essentially random.” '249 patent, col. 4:61–64. That disclosure refers to the '086 patent.

4 TriStrata has not adequately identified a structure that corresponds to claim 4. Although
5 the '249 and '086 patents disclose methods that involve using keys only once, they do not disclose
6 any structure for discarding the keys; they merely state that the keys are discarded. The Court
7 therefore finds that claim 4 is invalid as indefinite.

8 **IV. MOTION TO STRIKE TRISTRATA’S TECHNOLOGY TUTORIAL**

9 Following the Court’s denial without prejudice of Defendants’ ex parte motion to strike
10 portions of TriStrata’s technology tutorial, ECF No. 95, Defendants renewed their motion to
11 strike, and requested that the Court disregard pages 4, 5, 7, 8, 10, 12, 13, 15–17, and 28–30 of
12 TriStrata’s technology tutorial presentation, ECF No. 100 (Mot.), on the grounds that those pages
13 contain impermissible argument and violate this Court’s Order prohibiting TriStrata from
14 presenting the stricken expert testimony contained in the late-filed declaration of David Bernstein,
15 ECF No. 87 p. 5.

16 “[T]rial courts generally can hear expert testimony for background and education on the
17 technology implicated by the presented claim construction issues, and trial courts have broad
18 discretion in this regard.” Key Pharmaceuticals v. Hercon Laboratories Corp., 161 F.3d 709, 716
19 (Fed. Cir. 1998). See also, Markman, 52 F.3d at 980 (“The court may, in its discretion, receive
20 extrinsic evidence in order ‘to aid the court in coming to a correct conclusion’ as to the ‘true
21 meaning of the language employed’ in the patent.”) (quoting Seymour v. Osborne, 78 U.S. (11
22 Wall.) 516 (1871) (reviewing a decree in equity)). However, “if the meaning of a disputed claim
23 term is clear from the intrinsic evidence — the written record — that meaning, and no other, must
24 prevail; it cannot be altered or superseded by witness testimony or other external sources.” Id.

25 By agreement between the parties and order of the Court, the technology tutorial in
26 question did not become part of the record. Indeed, the Court typically does not receive on-the-
27 record technology tutorials, likely rendering any motion to strike portions of any tutorial moot.
28 Because the tutorial is not part of the official record of the case, an order to “strike” it would not

1 have any meaning. The motion is therefore denied.

2 For the same reason, the Court will deny Defendants’ motion with respect to the oral
3 presentation by expert witness David Bernstein at the parties’ tutorial presentation. Defendants
4 allege that Dr. Bernstein’s comments contained material from his stricken Second Declaration, as
5 well as improper argument concerning claim construction. Again, Dr. Bernstein’s comments were
6 not part of the record, and so there is nothing to “strike.” At least as importantly, and as
7 Defendants’ motion itself makes clear, the Court was quite capable of separating the wheat of Dr.
8 Bernstein’s comments from the chaff without the need for post-hearing motion practice. See ECF
9 No. 100 at 5 (“Indeed, Mr. Bernstein repeated this improper and tendentious assertion so many
10 times that the Court asked him to desist”).⁴

11 For these reasons, Defendants’ Motion to Strike is DENIED.

12 **V. CONCLUSION**

13 For the foregoing reasons, the Court construes the disputed claim language as follows:

Claim	Term	Construction
all claims	“seal”	“A data structure generated by a security server and containing a key or information to generate a key, wherein part or all of the data structure is encrypted and decrypted only by the security server that created it.”
’706 patent claims 2, 3, 4, 11, 14, 17, 18, 25, 28 ’249 patent claims 2, 3, 4	“key”	“A string of bits used in encryption to make data unreadable, or in decryption to render encrypted data readable.”

14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

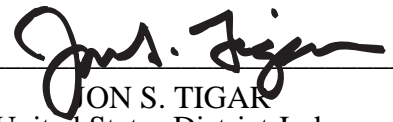
⁴ The Court repeats this comment from Defendants’ brief to demonstrate the lack of need for a motion, and not to adopt Defendants’ verbiage.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

'706 patent, claims 14, 28	“encrypt”	“To disguise information such that it is unreadable to anyone who does not have the key necessary to decrypt it.”
'706 patent, claims 1, 6, 16, 20, 25, 28 '249 patent, claims 1, 7	“information identifying who can access the document” “information identifying who can/one or more parties qualified to access the document”	Plain and ordinary meaning in view of the intrinsic record and knowledge of one of ordinary skill.
'706 patent, claims 13, 27 '249 patent, claim 13	“information which allows the computer system to confirm server identity”	“Information that allows the computer system to verify server identity information.”

IT IS SO ORDERED.

Dated: October 15, 2013



JON S. TIGAR
United States District Judge